REMARKS/ARGUMENTS

This Amendment is filed in response to the second, non-final Official Action issued following a Notice of Panel Decision from Pre-Appeal Brief Review re-opening prosecution of the present application. The second, non-final Official Action no longer rejects Claims 3 and 12-18 under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,775,772 to Binding et al. Instead, the Official Action rejects Claims 3 and 12-18 as being anticipated by newly-cited U.S. Patent No. 6,963,972 to Chang et al. In addition, the Official Action continues to reject the remaining claims, namely Claims 1, 2 and 4-11, under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,032,242 to Grabelsky et al., in view of U.S. Patent No. 6,356,529 to Zarom. As explained below, Applicant respectfully submits that the claimed invention is patentably distinct from Chang, Grabelsky and Zarom, and that at least Grabelsky and Zarom cannot reasonably be combined to disclose the claimed invention. Nonetheless, Applicant has amended various ones of the claims to further clarify the claimed invention, including amending independent Claim 3 to include the feature of dependent Claim 13. In view of the amendments to the claims and the remarks presented herein, Applicant respectfully requests reconsideration and allowance of all of the pending claims of the present application.

A.   Claims 3 and 12-18

The new, non-final Official Action rejects Claims 3 and 12-18 as being anticipated by Chang. Amended independent Claim 3 recites a system for providing network security, including means for receiving a request to perform a cryptographic operation, and means for returning a response to the cryptographic operation request. In addition, the system also includes means for translating a first plurality of cleartext data into a second plurality of cleartext data in accordance with one or more translation rules. The system further includes one or more modules for performing the cryptographic operations, including obtaining the first plurality of cleartext data based upon a first plurality of encrypted data, and encrypting the second plurality of cleartext data to obtain a second plurality of encrypted data. In this regard, as amended, the cryptographic operations are performed using cryptographic acceleration hardware.

In contrast to amended independent Claim 3, Chang does not teach or suggest at least

<u>performing cryptographic operations using cryptographic acceleration hardware</u>. Rejecting former dependent Claim 13, the Official Action cites column 6, lines 40-67 of Chang for allegedly disclosing cryptographic acceleration hardware. However, while one could argue that the cited passage of Chang discloses performing cryptographic operations, nowhere does the cited passage (or Chang in general) teach or suggest performing those operations using <u>cryptographic acceleration hardware</u>, as now recited by amended independent Claim 13.

Applicant therefore respectfully submits that amended independent Claim 3, and by dependency Claims 12 and 14-18, is patentably distinct from the system and method of Chang. As such, Applicant respectfully submits that the rejection of Claims 3 and 12-18 as being anticipated by Chang is overcome (or rendered moot by virtue of the cancellation of Claim 13).

B. *Claims 1, 2 and 4-11*

The Official Action also continues to reject Claims 1, 2 and 4-11 as being unpatentable over Grabelsky in view of Zarom. As previously explained, Grabelsky discloses a system and method for distributed network address translation with security features provided by Internet Protocol security protocol (IPsec). The distributed network address translation is accomplished with IPsec by mapping a local Internet Protocol (IP) address of a given local network device and a IPsec Security Parameter Index (SPI) associated with an inbound IPsec Security Association (SA) that terminates at the local network device. In a passage of Grabelsky cited in the Official Action, IPsec defines the security service Encapsulated Security Payload (ESP), and may be applied in a transport mode. In the transport mode, a sending endpoint may apply ESP to outbound packets in a manner including encapsulating information using a selected encryption technique (col. 23, ll. 27-39). Separately, a receiving endpoint may apply ESP to inbound packets in a manner including decryption using an encryption technique indicated by an appropriate security association (SA) (col. 23, l. 49 – col. 24, l. 4).

Zarom discloses a system and method for translating between data transmitted according to the WAP network protocols and data transmitted according to IP protocols. As disclosed, wireless communication devices that operate in accordance with WAP network protocols require a translation system, or gateway, to communicate with other devices that operate in accordance

with IP protocols. Zarom therefore discloses a system and method for WAP translation in a manner that enables a gateway translator to perform the translation process as soon as a minimal portion of data has been received.

According to a second aspect of the claimed invention, as reflected by independent Claim 1, a method for providing network security includes receiving a plurality of network protocol packets (e.g., IP packets). A network protocol packet includes a network protocol header (e.g., IP header) and a plurality of network protocol data, which includes a first cryptographic protocol header (e.g., TCP header) and a first plurality of encrypted data (e.g., SSL data). At least a portion of some of the network protocol packets are configured in accordance with a transport layer protocol (e.g., TCP/UDP) or a network layer protocol (e.g., IP). As also recited, a first plurality of cryptographic protocol rules (e.g., WTLS rules) associated with the network protocol data is determined, with a cryptographic session being established if required by the first cryptographic rules. The first plurality of cryptographic protocol rules are applied to the first encrypted data to obtain a first plurality of cleartext data (e.g., WML data). The first plurality of cleartext data is translated into a second plurality of cleartext data (e.g., HTML data) in accordance with at least one translation rule. The second plurality of cleartext data is then encrypted in accordance with at least one rule associated with a second cryptographic protocol (e.g., HTTP over SSL), resulting in a second plurality of encrypted data.

In contrast to the second aspect of the claimed invention, and as conceded in the Official Action, Grabelsky does not teach or suggest translating a first plurality of cleartext data into a second plurality of cleartext data. Nonetheless, the Official Action alleges that Zarom discloses this feature, and that one skilled in the art would have been motivated to modify Grabelsky to include the aforementioned feature of Zarom to teach the claimed invention. Applicant disagrees, however, and submits that even if Grabelsky and Zarom did disclose respective features of the claimed invention, one skilled in the art would not in fact have been motivated to modify Grabelsky to include the feature of Zarom to teach the claimed invention.

Initially, Applicant notes that the Official Action cites a passage of Grabelsky directed to a receiving endpoint applying ESP to inbound packets, and alleges that this passage reads on the claimed feature of applying a first plurality of cryptographic protocol rules to first encrypted data

to obtain a first plurality of cleartext data. The Official Action cites a passage of Grabelsky directed to a sending endpoint applying ESP to outbound packets, and alleges that this passage reads on the claimed feature of encrypting a second plurality of cleartext data into a second plurality of encrypted data. Then, the Official Action cites Zarom for disclosing a gateway translator translating between data transmitted according to the WAP network protocols and data transmitted according to IP protocols, and alleges that this passage reads on the intervening translation of the first plurality of cleartext data into the second plurality of cleartext data.

As explained in response to the last Official Action, taking the Official Action's interpretation of Grabelsky and Zarom as a given (although expressly not admitted), the combination of Grabelsky and Zarom teaches a receiving endpoint decrypting first encrypted data into a first plurality of cleartext data, a gateway translator then translating the first plurality of cleartext data into a second plurality of cleartext data, followed by a sending endpoint encrypting the second plurality of cleartext data into a second plurality of encrypted data. To effectuate the security services of Grabelsky, it only makes logical sense that the functions attributed to the receiving endpoint, gateway translator and sending endpoint are all performed by a single entity between endpoints within different networks (and thus needing address translation), such as by the router of Grabelsky. As disclosed by Grabelsky, however, the router does not modify the contents of received, secured (IPsec) packets since to do so would compromise the security of those packets. *See* Grabelsky, col. 3, l. 54 – col. 4, l. 3; col. 25, ll. 31-34; col. 32, ll. 45-46. Thus, even given the Official Action's interpretation of Gravelsky and Zarom (again expresssly not admitted) one skilled in the art would not be motivated to modify the end-to-end address translation with security of Grabelsky, with the translation of Zarom, to disclose the claimed invention.

In response to the foregoing, the Official Action notes that Grabelsky discloses overcoming the drawbacks of conventional network address translation (NAT) devices by implementing a distributed NAT (DNAT). Even considering Grabelsky's DNAT technique, and the alleged disclosure of Zarom, we still maintain that one skilled in the art would not have been motivated to modify the router of Grabelsky to include any translation attributed to Zarom. Again, Grabelsky clearly discloses that its router (router 26 of FIG. 1, "illustrating a network

system for distributed address translation" – col. 5, ll. 35-36) "does not modify contents of a received IPsec packet." Grabelsky, col. 32, ll. 45-46. And given the fact that Grabelsky explicitly does not modify the contents of a received packet so as to avoid compromising the security of that packet, one skilled in the art would not have been motivated to modify Grabelsky to translate a received packet, as alleged in the Official Action.

Applicant therefore respectfully submits that independent Claim 1, and by dependency Claims 4-11, is patentably distinct from Grabeksky and Zarom, taken individually; and respectfully submit that Grabeksky and Zarom cannot reasonably be combined to teach or suggest independent Claim 1, and by dependency Claims 4-11. Applicant also respectfully submits that independent Claim 2 recites subject matter similar to that of independent Claim 1. As such, Applicant respectfully submits that independent Claim 2 is patentably distinct from Grabeksky and Zarom for at least those reasons explained above with respect to independent Claim 1.

1. *Dependent Claims 6 and 9*

In addition to the aforementioned reasons, Applicant respectfully submits that various ones of dependent Claims 4-11 recite features that are further patentably distinct from Chang, Grabeksky and Zarom, taken individually or in combination. For example, dependent Claims 6 and 9 further recite that the first and second cryptographic protocols comprise WTLS and SSL over HTTP, respectively. The Official Action cites both Grabelsky and Zarom for allegedly disclosing the feature of Claim 6, citing column 7, lines 10-12 of Grabelsky and column 3, lines 5-6 of Zarom for disclosing WTLS; and cites Zarom for allegedly disclosing the feature of Claim 9, citing column 8, lines 7-11 for disclosing SSL over HTTP. Applicant respectfully submits, however, that not only do none of these passages disclose the features to which they are attributed, but no other passage of Grabelsky or Zarom disclose those features.

For at least the foregoing reasons, Applicant respectfully submits that the rejection of Claims 1, 2 and 4-11 as being unpatentable over Grabelsky, in view of Zarom, is overcome.
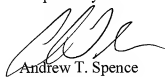
CONCLUSION

In view of the amendments to the claims and the remarks presented above, Applicant respectfully submits that the present application is in condition for allowance. The issuance of a Notice of Allowance is therefore respectfully requested. In order to expedite the examination of the present application, the Examiner is encouraged to contact Applicant's undersigned attorney in order to resolve any remaining issues.

It is not believed that extensions of time or fees for net addition of claims are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 CFR § 1.136(a), and any fee required therefore (including fees for net addition of claims) is hereby authorized to be charged to Deposit Account No. 16-0605.

Respectfully submitted,

Andrew T. Spence
Registration No. 45,699

Customer No. 00826
ALSTON & BIRD LLP
Bank of America Plaza
101 South Tryon Street, Suite 4000
Charlotte, NC 28280-4000
Tel Charlotte Office (704) 444-1000
Fax Charlotte Office (704) 444-1111

ELECTRONICALLY FILED USING THE EFS-WEB ELECTRONIC FILING SYSTEM OF THE UNITED STATES PATENT & TRADEMARK OFFICE ON NOVEMBER 19, 2007.

LEGAL02/30602184v1